# 重置管理员用户的密码Cisco Firepower系统的

## Contents



## Introduction

本文为重置密码提供指令在FireSIGHT、Firepower和ASA Firepower服务工具，包括在该密码丢失了的情况。防御中心和Firepower管理中心提供不同的(用独立的密码)命令行界面(CLI) /shell访问和Web接口访问的(当可得到时)。在可管理的设备的是相同的为CLI访问、shell访问和Web接口访问(当可得到时。)

这些指令援引Firepower管理中心;同样指令适用于防御中心。

> **Note**:在Firepower管理中心CLI的参考仅适用于版本6.3+。

## 更改CLI或Shell管理员密码FMCs、7000和8000系列设备和NGIPSv的

请使用这些指令重置以下已知密码：

- Firepower访问的CLI或shell
- 7000和8000系列设备： 用于的访问Web接口，以及CLI
- NGIPSv 用于的访问shell

**程序：**

1. 日志到工具里通过SSH使用。
   •默认情况下对于Firepower管理中心，这提供您对shell的访问。如果Firepower管理中心CLI是启用的，这提供您对CLI的访问。
   •对于可管理的设备这提供您对设备CLI的访问。

2. 对于可管理的设备，或者有CLI功能的一个Firepower管理中心的，请输入命令访问shell。

3. 在shell提示请输入以下命令：
   ```
   sudoadmin
   ```

4. 当提示，请输入当前举起权限到根访问权限。

5. 以回应提示，两次请输入新的。
   **Note**:如果系统显示消息，这只是与信息有关的。系统运用您供应的密码，即使此消息出现。然而， Cisco建议由于安全原因您使用一个复杂密码。
6. 键入退出shell。

7. 在一个可管理的设备上，或者在有CLI功能的一个Firepower管理中心，请键入退出CLI。

# 更改FMCs和7000和8000系列设备的Web接口管理员密码

请使用这些指令重置以下已知密码：

- Firepower用于的访问Web接口
- 70008000用于的访问Web接口，以及CLI

**程序：**

1. 日志到工具里通过SSH使用。
   •默认情况下对于Firepower管理中心这提供您对shell的访问。如果Firepower管理中心CLI是启用的，这提供您对CLI的访问。
   •对于可管理的设备这提供您对设备CLI的访问。

2. 对于可管理的设备，或者有CLI功能的一个Firepower管理中心的，请输入命令访问shell。

3. 在shell提示请输入以下命令：
   `sudo usertool.pl - p ‘’`
   那里是期望新的密码。

4. 键入退出shell。

5. 在一个可管理的设备上，或者在有CLI功能的一个Firepower管理中心，请键入退出CLI。

# 重置丢失的CLI或Shell管理员密码FMCs、7000和8000系列设备和NGIPSv的

请使用这些指令重置以下一个丢失的密码：

- Firepower用于的访问CLI或shell
- 70008000用于的访问Web接口，以及CLI
- NGIPSv 用于的访问shell

**Note**:重置您需要建立与工具的一个控制台连接的这些一个丢失的密码。您也需要重新启动`admin`证件您丢失的工具。您可以根据什么类型的设备访问起动重新启动用不同的方式，您把可用：

•对于Firepower管理中心您需要一个Web接口用户的登录证件有管理员访问的。
•对于7000或8000系列设备您需要的登录证件访问任一个下列的平均值：有管理员访问的一个Web接口用户，有配置访问的一个CLI用户或者有管理员访问的一个用户在管理Firepower管理中心。
•对于NGIPSv您需要一个CLI用户的登录证件有配置访问的或者有管理员访问的一个用户在管理Firepower管理中心。

如果不能访问有那些方法之一的设备，您不能重置与这些指令的;联系Cisco TAC。

**程序：**

1. 打开与工具控制台的连接您丢失了的设备的：
   • 对于7000系列设备， 8000系列设备和Firepower管理中心使用关键董事会/监控程序连接，指定设备的主机名或管理接口的IP地址为工具。
   •对于虚拟工具请使用VMware控制台。请参阅虚拟Cisco Firepower的管理中心关于VMware配置快速入门指南欲知更多信息。

2. 重新启动您丢失了的设备。您有以下选择：
   •Firepower管理中心：
   A. 日志到Firepower管理中心的Web接口里作为用户与管理员访问。
   B. 重新启动Firepower管理中心正如您的版本Firepower管理中心配置指南所描述。

   •7000或8000系列设备或NGIPSv，如果有一个Web接口用户的证件有在管理Firepower管理中心的管理员访问的：
   A. 日志到管理Firepower管理中心的Web接口里作为用户与管理员访问。
   B. 关闭并且重新启动可管理的设备正如您的版本Firepower管理中心配置指南所描述。

   •7000或8000系列设备，如果有一个Web接口用户的证件有管理员访问的：
   A. 登陆对设备的Web接口作为用户与管理员访问。
   B. 重新启动设备正如您的版本Firepower管理中心配置指南所描述。

   •7000或8000系列设备或NGIPSv，如果有一个CLI用户的证件有配置访问的：
   A. 日志到工具里通过shell使用与CLI配置访问的一个用户名。
   B. 在提示，请输入`reboot`。
   **Note**:当您重新启动您的Firepower管理中心或可管理的设备时，这注销您在您的工具外面，并且系统进行能占去1小时完成的数据库检查。**警告：**使用功率按钮，请勿关闭工具，或者通过拔掉电源电缆;它可能破坏系统数据库。使用Web接口，完全地关闭工具。
3. 在工具控制台显示，请观察重新启动进程并且根据重新启动的工具的种类进行：
   **Note**:如果系统执行数据库检查，您可以发现下列信息：•对于Firepower Firepower 7000或8000系列设备或NGIPSv的管理中心型号750， 1500， 2000， 3500或者4000，或者，请中断重新启动进程：
   A.一旦工具开始启动，请按在您的关键董事会的所有键取消读秒在LILO引导程序菜单。
   B.注释在LILO引导程序菜单显示的版本号。在下面的示例中版本号是`6.2.0`。


C. 在提示，键入version命令是版本号的地方(例如6.2.0)。

- Firepower管理中心型号1000， 2500或者4500 ：
  当引导程序菜单出现时，请选择选项4， Cisco Firepower管理控制台密码恢复模式。

4. 当系统显示与#符号的一个OS提示结束(#)，请输入passwd命令admin。

5. 输入新的当提示如此执行(两次)。
   **Note**:如果系统显示消息，这只是与信息有关的。系统运用您供应的密码，即使此消息出现。然而， Cisco建议由于安全原因您使用一个复杂密码。
6. 在与#符号的OS提示结束(#)，请输入reboot

7. 允许重新启动进程完成。

# 重置FMCs和7000和8000系列设备的丢失的Web接口管理员密码

请使用这些指令更改以下密码：

- Firepower用于的访问Web接口
- 70008000用于的访问Web接口，以及shell

**程序：**

1. 打开与工具的连接访问shell登录提示：
   •对于7000系列设备， 8000系列设备和Firepower管理中心，使用关键董事会/监控程序或者串行连接，指定主机名-设备或管理接口的IP地址工具的。
   •对于虚拟Firepower管理中心使用VMware控制台。请参阅虚拟Cisco Firepower的管理中心关于VMware配置快速入门指南欲知更多信息。

2. 在prompt命令，输入用户名。
   •对于Firepower管理中心，请输入admin。
   •对于7000和8000系列设备，请输入与CLI配置访问的一个用户名。

3. 在提示，输入密码。

4. 对于可管理的设备或有CLI功能的一个Firepower管理中心的，在CLI提示，请输入命令退出CLI和访问shell。

5. 在shell提示，请输入以下命令重置Web接口密码：
   `sudo usertool.pl -p ''`
   那里是新的密码。

6. 在提示，输入您当前登陆的用户名的密码。

7. 键入退出shell。

8. 在一个可管理的设备上或在有CLI功能的一个Firepower管理中心，请键入退出CLI。

# 重置Firepower威胁防御设备的丢失的管理员密码

要重置一个Firepower威胁防御(FTD)逻辑设备的在Firepower 9300和4100平台，您能遵从在更改的指令或通过FXO机箱管理器指南恢复FTD的密码。

对于运作在Firepower 2100的FTD设备，您必须再镜像设备。请参阅Cisco FXO故障排除指南关于重新镜像程序的Firepower 2100系列运行的Firepower威胁防御在此平台。

对于运作在ASA5500-X和ISA 3000型号的FTD设备，您必须再镜像设备。请参阅Cisco ASA和Firepower威胁防御设备重新镜像指南关于指令。

再镜像设备清除其配置并且重置对`Admin123`。

- 如果再镜像用Firepower设备管理器管理的FTD设备： 如果有一最近，外部存储的备份，您能恢复被备份的配置，在您再镜像后。欲知更多信息请参阅*Cisco Firepower威胁防御配置指南关于Firepower*您的版本的(https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html)*设备管理器*。如果没有备份您必须手工再创设备配置，包括接口、路由策略和DHCP和DDNS设置。
- 如果再镜像FTD设备管理与Firepower管理中心： 如果FMC和设备运行版本6.3+，您能使用FMC Web接口备份设备配置，在您再镜像前，并且恢复备份，在您再镜像后。欲知更多信息，请参阅Firepower管理中心配置指南关于您的版本。
  **Note**:从FMC Web接口的备份和恢复不为FTD容器实例支持。如果运行一个更早版本，您不能备份设备配置。虽然您能从Firepower管理中心运用共享策略，在您再镜像后，您必须手工配置任何东西设备特有，例如接口、路由策略和DHCP和DDNS设置。

# 重置在ASA Firepower服务模块的管理员密码

使用`session`ASA一般操作CLI，您能重置ASA Firepower模块CLI的管理员密码。 如果丢失了ASA CLI的密码，您能恢复他们正如CLI书1所描述：Cisco ASA系列一般操作CLI您的ASA版本配置指南。

## 重置在ASA 5512-X的管理员密码通过ASA 5555-X和ASA 5506-X通过ASA 5516-X设

## 备(软件模块)

要重置ASA Firepower软件模块的到默认密码请输入此at命令ASA提示：

```
sfr
```

欲知更多信息，请参阅Cisco ASA系列CLI书2 ：Cisco ASA系列防火墙CLI您的ASA版本配置指南。

## 重置在ASA 5585-X系列设备(硬件模块)的管理员密码

要重置ASA Firepower硬件模块的到默认密码请输入此at命令ASA提示：

```
1
```

欲知更多信息，请参阅Cisco ASA系列CLI书2 ：Cisco ASA系列防火墙CLI您的ASA版本配置指南。